

CLERK'S OFFICE

A TRUE COPY

Jan 07, 2021

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information in the possession of Microsoft Corporation and associated with
OneDrive User ID "30000301e2889." This information is stored at premises
owned, maintained, controlled, or operated by Microsoft Corporation, an electronic
communications service headquartered at 1 Microsoft Way, Redmond, WA 98052.

Case No. 21 MJ 10

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the
property to be searched and give its location)*:

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the
person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

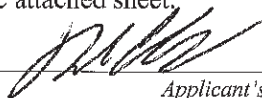
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 2252 and 2252A	Possession and distribution of child pornography

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



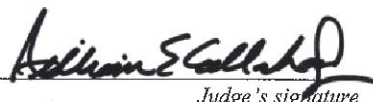
Applicant's signature

FBI Task Force Officer Daniel K. Chmielewski

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*.

Date: January 7, 2021



Judge's signature

City and state: Milwaukee, Wisconsin

Hon. William E. Callahan, Jr., U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Daniel Kenneth Chmielewski, being first duly sworn, herby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for all information associated with the OneDrive account that is stored at premises owned, maintained, controlled or operated by Microsoft Corporation (hereinafter “Microsoft”), located at One Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I am a Task Force Officer (TFO) with the United States Department of Justice, Federal Bureau of Investigation (FBI), for the Child Exploitation and Human Trafficking Task Force. I have been employed as a law enforcement officer since 2013 and have been assigned as a TFO since March 2020. I am currently employed as a Detective with the Waukesha County Sheriff’s Department and am assigned to the computer forensics lab. As such, I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, U.S.C. § 2510 (7). That is, I am an officer of the United States, who is empowered by law to conduct investigations regarding violations of United States law, to execute warrants issued under the authority of the United States, and to make arrests of the offenses enumerated in Title 18,

U.S.C. § 2251, *et. seq.* In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation, child abductions, and child pornography investigations. I have previously been involved in criminal investigations concerning violations of federal and state laws.

3. Since joining law enforcement, your affiant has received specialized training in child pornography investigations, identifying and seizing electronic evidence, computer forensics, recovery, and social media investigations. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

5. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

6. Title 18 U.S.C. § 2256(2)(A) defines “sexually explicit conduct” as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or the lascivious exhibition of the genitals or pubic area of any person.

7. “Visual depictions” include data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (*See* 18 U.S.C. § 2256(5)).

8. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital to genital, oral to genital, or oral to anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. (*See* 18 U.S.C. § 2256(2)).

9. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, see *United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App’x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), *aff’d sub nom, United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff’d*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987).

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

COMPUTERS AND CHILD PORNOGRAPHY

11. The Internet and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To

distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these was accomplished through a combination of personal contacts, mailings, and telephone calls.

12. The development of computers and the Internet, including smart phones which act as computers, have changed this paradigm. Computers serve four basic functions in connection with child pornography, namely, production, communication, distribution, and storage.

13. Child pornographers can now transfer photographic prints made from a film camera into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly from a digital camera onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally hundreds of millions of computers around the world.

14. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

15. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's

computer. Graphic image files containing child pornography can be maintained for long periods of time on a computer or electronic storage.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

16. I know based on my training and experience that most individuals who are sexually attracted to children facilitate their sexual arousal through imagery that focuses, in part or in whole, on children. Specifically, these individuals often collect child pornography. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed depictions of children engaged in nonsexual activity to nude or partially nude depictions of children engaged in sexually explicit conduct.

17. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, drawings, cartoons and non-sexually explicit visual images of children.

18. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting

and organizing their child related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other likeminded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

19. Persons with a sexual interest in children often maintain and possess their material in the privacy and security of their homes or some other secure location, such as a private office or work computer, where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images, computer videos, or other visual media. Because they put so much time and energy into obtaining the material, they do not delete or destroy their collections.

20. Your affiant is also aware that those who possess child pornography often communicate and trade child pornography with other likeminded criminals over the internet or through other electronic means.

BACKGROUND RELATING TO ONEDRIVE

21. Microsoft provides a variety of online services to the general public. One of those services is Microsoft OneDrive, which is a cloud storage service that allows an individual store

personal files in one place, share those files with others, and access those files from any device connected to the internet. OneDrive was previously known as SkyDrive.

22. Users of OneDrive do not need to have an email account provided by Microsoft in order to use Microsoft OneDrive. Users can open a Microsoft OneDrive account with any email address.

23. Microsoft OneDrive allows users to upload files, photos and favorites on Microsoft servers, to cloud storage, and allows members to access them from any computer with an internet connection. After uploading photos and/or files to OneDrive, users can share the photos and files that they create with others. The user can send an email to other individuals inviting them to view the photos and files. The service allows the user to keep the files private, share with contacts, or make the files public. Publicly shared files do not require a Microsoft ID to access; the service offers five gigabytes of free personal storage. Additional personal storage can be purchased by the user.

24. In general, companies that provide cloud storage accounts like Microsoft maintain subscriber information for its customers to include certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, email addresses, and business information. Microsoft may also retain records of the length of service and types of services utilized. In addition, for paying customers, Microsoft may likely retain information about the customer's means and source of payment for services (including a credit card or bank account number).

25. Microsoft maintains server computers connected to the Internet. To upload files to OneDrive, customers may place files and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur

in several ways. Servers often maintain logs of these connections, showing the dates and times of the connection, the method of connecting and the Internet Protocol addresses (“IP addresses”) of the remote users’ computers. Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data.

26. In some cases, a subscriber or user will communicate directly with Microsoft about issues relating to an account, such as technical problems, billing inquiries, or complaints from other users. Microsoft may retain records about such communications, including records of contacts between the user and the company’s support services, as well as records of any actions taken by the company or user as a result of the communications.

27. As Microsoft hosts the Subject Account, it is likely the computers of Microsoft contain the material just described, including stored electronic communications and information concerning subscribers and their use of Microsoft OneDrive, such as account access information, transaction information and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Microsoft, to protect the rights of the subject investigation and to effectively pursue this investigation, authority is sought to allow Microsoft to make a digital copy of the entire contents of the information subject to seizure specified in Attachment B.

28. OneDrive is a cloud storage service owned and operated by Microsoft Corporation and headquartered in Redmond, Washington. OneDrive offers users the ability to store files remotely, to include images, videos, and documents. A user can access these files by logging into their account on an internet connected device, such as a cellphone, tablet, or computer. OneDrive

also allows the user to share files with other users by sending a link which will allow other users to access their files and/or folders.

29. The basic OneDrive service is free and allows users to store up to 5GB of files. For \$1.99 per month, users can increase their storage limit to 100GB. For \$6.99 per month, a user can enroll in Microsoft 365 Personal, which gives a user 1 Terrabyte of storage, and the use of Microsoft Office tools, such as Microsoft Word, Excel, Powerpoint, and Outlook Email. For \$9.99 per month, a user can enroll in Microsoft 365 Family, which gives the account holder 6 Terrabytes of storage total (1 Terrabyte per user in the family) and use of the Mircrosoft Office tools described above.

DEFINITIONS/TECHNICAL TERMS

30. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure

of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

d. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

e. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

f. “Child Pornography” means the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the

visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2)(8).

g. “Computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).

h. “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

i. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption

devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. “Computer-related documentation” means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

l. “Domain Name” means the common, easy-to-remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level read backwards – from right to left – further identifies parts of an organization. Examples of first-level or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely

identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Internet Connection” means a connection required for access to the Internet. The connection would be provided by cable, DSL (Digital Subscriber Line) or satellite systems.

n. “Internet Service Providers” or “ISPs” mean commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

o. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

p. A “modem” translates signals for physical transmission to and from the Internet Service Provider, which then sends and receives the information to and from other computers connected to the Internet.

q. A “router” often serves as a wireless access point and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. The router is in turn typically connected to a modem.

r. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

s. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

t. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

u. “Wireless network” as used herein means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. But, if wireless access points are connected to the network, anyone

in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

v. “Secure Hash Algorithm Version 1 hash value” (SHA 1 hash value) is an algorithm that processes digital files, resulting in a 160-bit value that is unique to that file. It is computationally infeasible for two files with different content to have the same SHA 1 hash value. By comparing the hash values of files, it can be concluded that two files that share the same hash value are identical with a precision that exceeds 99.9999 percent certainty. There is no known instance of two different child pornographic images or videos having the same SHA1 hash value.

w. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to set up files on a computer to be shared with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network. However, a tool used by law enforcement restricts

the download so that the file is downloaded, in whole or in part, from a single user on the network.

1. When a user wishes to share a file, the user adds the file to his a shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's SHA 1 has value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

2. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

NCMEC CYBERTIPLINE

31. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their CyberTipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These CyberTipline reports are reviewed by a NCMEC analyst and forwarded to Law Enforcement for further investigation on the information provided in the CyberTipline report. ISPs, ESPs, and others may physically view a picture, video, or any other content that they would then report to NCMEC.

PROBABLE CAUSE

32. On July 20, 2020, Microsoft completed a Cybertip to NCMEC. The Cybertip number was **74930637**. Microsoft reported that a OneDrive account with an electronic service provider user ID number of, "30000301e2889," uploaded 25 files, which Microsoft classified as apparent child pornography on July 19, 2020, at 22:40 hours (UTC). The files were not reviewed by NCMEC or Microsoft but were classified based on hash value.

33. I know from my training and experience that the ISP flags and reports images or files that have the same “hash values” as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is similar to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

34. I know from my training and experience that the ISP compares the hash values of files that its customers transmit on its systems against the list of hash values that NCMEC has. If the ISP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ISP's systems.

35. I also know that the ISP uses PhotoDNA. PhotoDNA is a software technology developed by Microsoft that computes hash values of images, video and audio files to identify like images. PhotoDNA is primarily used in the prevention of child pornography proliferation. Here, that technology was used to determine that a user of its services posted or transmitted a file with the same hash value as an image that has previously identified as containing child pornography.

36. The IP address associated with the OneDrive uploads was 184.58.138.130. Based on the geo-location of the IP address, NCMEC forwarded the tip to the Wisconsin Department of Justice Department of Criminal Investigations (DCI). DCI conducted an administrative subpoena to Charter Communications and located a subscriber name of Larry Theurich, with an address of

W303 S2789 Bethesda Circle in the Town of Genesee, Waukesha County, Wisconsin. Based on the address, DCI forwarded the information to the Waukesha County Sheriff's Department (WKSD), which is an internet crimes against children affiliate agency.

37. On September 9, 2020, WKSD Detective Mark Conrad received and reviewed **CyberTip 74930637**. Detective Conrad reviewed the uploaded photograph files in question and provided the following details:

38. "... I also reviewed the images attached to the tip. I noted that all 25 files appear to show apparent child pornography. Two images of note are described as an infant female being sexually assaulted with a screwdriver and a ballpoint pen or marker. Another image depicts an adult male sexually assaulting an infant female. The other images contained within the tip depicts similar images of both male and female children being sexually assaulted and/or exposing their genital areas."

39. During the course of the investigation, Detective Conrad found that Larry has a brother named, Eric P. Theurich, and that Eric had registered a vehicle at the above address. Detective Conrad further found out that Eric is a convicted sex offender, had recently served time in prison for possession of child pornography, and was on parole.

40. Detective Conrad made contact with Eric's parole agent, Jennifer Uppena, who stated that Eric is on active GPS monitoring and that he resides at a location called, "Cesar's Inn," located at 5527 W. National Avenue in West Milwaukee, Milwaukee County, Wisconsin. Jennifer stated that Eric stays every 7 to 10 days at Larry's residence in the Town of Genesee. Jennifer checked the GPS records for Eric and found that on the day of the illegal uploads, July 19, 2020, Eric was at Larry's residence in the Town of Genesee, Waukesha County, Wisconsin.

41. TFO Chmielewski wrote a federal search warrant to view the Cybertip contents.

After obtaining the warrant, TFO Chmielewski reviewed the contents of the Cybertip. All of the images clearly depict child sexual abuse material (CSAM). The follow are descriptions of three of the files.

42. File Name: 35cf4acd-5f62-4c92-a755-13309a6f97ea.jpeg

This image is a color photograph of a Caucasian female baby, approximately one years-old. The baby is wearing a white shirt and does not have clothing on the bottom half of her body. The baby's feet and legs are up in the air, showcasing her vagina and anus area. An adult male's feet are on the baby's thighs, keeping her legs elevated. A screwdriver with a green handle is inserted inside of the baby's anus. The adult male is also inserting a pink pencil into the baby's vagina.

43. File Name: 6a90ae90-88cb-4796-ace7-17b465c28dca.jpeg

This image is a color photograph of a Caucasian prepubescent female, approximately 3-5 years old. The juvenile is wearing a denim dress and a black and white striped long-sleeve shirt. The juvenile is laying on her back and has her legs in the air, holding her legs up with her hands. The juvenile is not wearing any pants and is clearly showing her vagina and anus. The juvenile's diaper is located on her ankles, in the air.

44. File Name: 68cf1787-dd0f-4924-a2d5-685b713d99df.jpeg

This image is a color photograph of a Caucasian prepubescent female, approximately 3-5 years old. The juvenile is completely nude, laying on her back, on top of a tan comforter. The juvenile has a pink pacifier in her mouth and is using both her left and right hands on the outer portion of her vagina to show the camera the inner canal of her vagina. The juvenile's anus area is also seen in the photograph.

INFORMATION TO BE SEARCHED

45. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B.

CONCLUSION

46. Based on the forgoing, I request the Court issue the proposed search warrant for records. Since the warrant will be served on Microsoft who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to be searched

This warrant applies to information in the possession of Microsoft Corporation and associated with OneDrive User ID “30000301e2889.” This information is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an electronic communications service headquartered at 1 Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

I. INFORMATION TO BE DISCLOSED BY MICROSOFT CORPORATION

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft Corporation, Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A, for any available time period until the present date:

- a. The content of any and all cloud storage and other accounts;
- b. All records or other information regarding the identification of the accounts described in Attachment A above, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP address associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) provided by the subscriber to Microsoft;
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, to include any and all contacts listed on the subscriber's contact list, pictures, and files, to include any and all contents of electronic files that the subscriber has stored; and
- d. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of action taken.
- e. Any additional information Microsoft has in regards to CyberTipline Report Number "74930637."

II. INFORMATION TO BE SEIZED BY GOVERNMENT

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, §§ 2252 and 2252A, including the following:

- a. All files, documents, communications, images, videos, contacts, metadata, and logs associated with OneDrive user ID “30000301e2889”; related to visual depictions of minors engaging in sexually explicit conduct or child pornography, in violation of Title 18, United States Code § 2252 and 2252A, along with any evidence that would tend to show the true identities of the persons committing these offenses.
- b. All activity logs and IP logs, including all records of the IP addresses that logged into the account
- c. All account information, including:
 - i. All registration, identity, and contact information, including full name, email addresses, physical addresses (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
 - ii. The length of the service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number(s));
 - iii. All privacy settings and other account settings;
 - iv. All registered devices and accompanying serial numbers, IMEI number, make and model information, and other identifying numbers to include dates of activation, registration, deactivation; and
 - v. All records pertaining to communications between Microsoft Corporation

and any person regarding the user or the user's OneDrive account, including contacts with support services and records of actions taken.

III. METHOD OF DELIVERY

Items seized pursuant to this search warrant should be served by sending all electronic information in its original electronic form, on any digital media device, email, via US Postal Service or another delivery service – notwithstanding 18 U.S.C. §§ 2251, 2252, and 2422, or similar statutes or codes – to the email, dkchmielewski@fbi.gov and/or the physical address of:

FBI Milwaukee
Attention: TFO Daniel Chmielewski
3600 S. Lake Drive,
St. Francis, WI, 53235